Docket No. 212/688US

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

In re Application of:	
Chen, et al.	
Serial No.: 10/524,057	Art Unit: 2431
Filed: December 29, 2005	Confirmation No.: 4440
For: Distributed Processing in Authentication	Examiner: Wright, Bryan F.

RESPONSE TO OFFICE ACTION

MS Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This paper is responsive to the Office Action dated May 20, 2010 and the Advisory Action dated September 23, 2010. A Request for Continuing Examination is filed along with this amendment.

Certificate of transmission under 37 CFR 1.8

I hereby certify that this response (along with any paper referred to as being attached or enclosed) is being transmitted to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

FILED VIA EFS
Date: November 22, 2010

/Paul J. Backofen/
Paul J. Backofen, Esq., 42278

Claim Listing:

1. (previously amended) A method of authenticating a user according to a biometric parameter of the user presented at an authentication device on a user-presented device on which is stored a biometric identification template divided into a secure portion and an open portion, the method comprising:

transmitting to a client terminal data derived from said user biometric parameter at the authentication device;

transmitting from a user-presented device to the client terminal only the open portion of the said biometric identification template held on the user-presented device, wherein the open portion is the portion containing data insufficient to construct a fake template that would allow an impostor to be incorrectly authenticated as a genuine user and comprises parameters of a predetermined number of unique features of the template;

at the client terminal, implementing a first stage of a biometric identity authentication process between said derived data and said open portion to produce intermediate results, and transmitting the intermediate results of said biometric authentication process to the user-presented device, wherein said intermediate results comprise parameters for alignment of said derived data and said biometric identification template; and

at the user-presented device implementing a second stage of the biometric identity authentication process to complete the biometric identity authentication process using said

intermediate results and said secure portion and issuing a biometric authentication result based thereon.

2. (previously amended) A method of registration of a user according to a biometric parameter of the user presented at an authentication device, the method comprising:

transmitting to an authorized client terminal data derived from said user biometric parameter obtained at the authentication device;

at the authorized client terminal, dividing the biometric identification template computed into secure portion and open portion, wherein the open portion is the portion containing data insufficient to construct a fake template that would allow an impostor to be incorrectly authenticated as a genuine user and comprises parameters of a predetermined number of unique features of the template;

transmitting from the authorized client terminal to a user-presented device both the open portion and the secure portion of a biometric identification template,

storing the said template consisting of open and secure portions on the user-presented device, with the secure portion only accessible within the user-presented device and not externally.

3. (previously amended) A method according to claim 1, wherein the secure portion of the biometric identification template is the portion containing data unauthorized modification of which

may cause an impostor to be incorrectly authenticated as a genuine user.

4. (cancelled)

5. (previously amended) A method according to claim 1, wherein the biometric parameter is a fingerprint.

6. (cancelled)

7. (previously amended) A method according to claim 1, wherein the first stage of said biometric identity authentication process implemented at the client terminal comprises locating unique features using the data derived from the user biometric parameter and aligning them with said predetermined number of unique features from the identification template held on the user-presented device.

8. (previously presented) A method according to claim 1, wherein the second stage of the said identity authentication process implemented on the user-presented device is implemented using a local executable matching program stored on the device.

9. (previously presented) A method according to claim 1, wherein the first stage of the identity authentication process implemented at the client terminal is implemented using a client executable matching program.

10. (original) A method according to claim 9, wherein the client executable matching program is stored on the user-presented device or the authentication device and is transmitted to the client terminal at the time of authentication.

11. (original) A method according to claim 9, wherein the client executable matching program is downloaded by the client terminal from a remote memory at the time of authentication.

12. (previously presented) A method according to claim 1 wherein the authentication result is used to authenticate a user for authorizing a secure transaction.

13. (original) A method according to claim 12, wherein the secure transaction is controlled by an executable transaction program stored on the user-presented device.

14. (previously presented) A method according to claim 1, wherein, when the authentication result indicates an adequate match, a first security access check key is constructed including the authentication result.

15. (previously presented) A method according to claim 13 , wherein a second security access check key is requested and compared with the first security access key, the result of said comparison being used to enable the executable transaction program if it yields a positive authentication result.

16. (original) A method according to claim 15, wherein the second security access check key is issued from a security server.

17. (previously presented) A method according to claim 16, wherein the first and second security access check keys each include a unique identification number.

18. (previously presented) A method according to claim 15, wherein the unique identification number contains a number

obtained from a mathematical operation on a randomly generated number and the authentication result.

19. (original) A method according to claim 18, wherein the randomly generated number changes at each time the number is used.

20. (original) A method according to claim 19, wherein the changing random number is tracked by dividing the number into two portions, a first portion to be used as the current random number and a second portion to be used as the next random number.

21. (previously presented) A method according to claim 17, wherein the unique identification number contains a number that is remembered by the user.

22. (previously presented) A method according to claim 18, wherein more than one authentication methods can be used to obtain the authentication result, each being incorporated into the unique identification number.

23. (previously presented) A method according to claim 17, wherein the access is divided into several levels and wherein the level of access granted to a user is dependent on the confidence level of positive identity obtained from the unique identification number.

24. (previously amended) A system for authenticating a user according to a biometric parameter of the user, the system comprising:

a user-presented device on which is stored a biometric identification template divided into a secure portion and

an open portion, wherein only said open portion can be transmitted out of the said device, wherein the open portion is the portion containing data insufficient to construct a fake template that would allow an impostor to be incorrectly authenticated as a genuine user and comprises parameters of a predetermined number of unique features of the template;

an authentication device operable to read biometric data derived from a user, and comprising means for communicating with the user-presented device and a client terminal;

a client terminal arranged to receive the said open portion of the biometric identification template held on the user-presented device and the biometric data derived from the user, and comprising a client processor operable to implement a first stage of a biometric identity authentication process between said derived data and said open portion to produce intermediate results, and to transmit the intermediate results of said biometric identity authentication process to the user-presented device, wherein said intermediate results comprise parameters for alignment of said derived data and said biometric identification template;

and wherein the user-presented device comprises a device processor operable to implement a second stage of the biometric identity authentication process to complete the biometric identity authentication process using said intermediate results and said secure portion to issue a biometric authentication result based thereon.

25. (previously amended) A system according to claim 24, wherein the secure portion of the biometric identification template is the portion containing data unauthorized modification of which may cause the system to incorrectly authenticate an impostor as a genuine user.

26. (cancelled)

27. (previously amended) A system according to claim 24, wherein the biometric parameter is a fingerprint, and wherein the authentication device includes a fingerprint sensor.

28. (cancelled)

29. (previously presented) A system according to claim 24, wherein the user-presented device comprises a memory in which is stored a local executable matching program for implementing the second stage of the matching process.

30. (original) A system according to claim 29, wherein the memory on the user-presented device stores a client executable matching program which is transmitted to the client processor to implement the first stage of the matching process.

31. (previously presented) A system according to claim 24, which comprises a security server connected to the client terminal.

32. (original) A system according to claim 31, wherein the security server holds a client executable matching program for implementing the first stage of the matching process.

33. (previously presented) A system according to claim 31, wherein the security server holds a security access check key requestable by the client terminal for enabling a transaction.

34. (previously presented) A system according to claim 24 , which comprises a transaction server arranged to implement secure transactions and which is in communication with the client terminal so that the authentication result is usable to authenticate a user for authorizing a secure transaction.

35. (original) A system according to claim 34, wherein the user-presented device stores an executable transaction program for controlling the secure transaction.

36. (previously presented) A system according to claim 34, wherein more than one authentication methods can be used to obtain the authentication result.

37. (previously presented) A system according to claim 34, wherein the access to the transaction server is divided into several levels and wherein the level of access granted to a user is dependent on the confidence level of positive identity obtained based on the results from the various authentication methods used.

38. (previously amended) A method of executing an operation using first and second processors, the method comprising:

storing in the first processor a first task table containing a plurality of process names with associated process identifiers, each associated with a process locator;

storing in the second processor a second task table containing said of process names and process identifiers;

identifying at the second processor a process to be executed and issuing a request to the first processor to execute said process;

locating said process using the process locator and executing said process at the first processor to generate a result; and

returning the result to the second processor;

wherein the operation being executed is a fingerprint-matching algorithm comprising a base minutiae finding process executed by the first processor and a minutiae matching process executed by the second processor,

wherein the base minutiae finding process is a first stage of a biometric identity authentication process implemented between data derived from a user biometric parameter and an open portion of a biometric identification template, wherein the biometric identification template is divided into the open portion and a secure portion, to produce intermediate results, said open portion containing a subset of minutiae data selected such that the content of the open portion is insufficient to construct a fake template that would allow an impostor to be incorrectly authenticated as a genuine user, and said intermediate results comprise parameters for alignment of said data and said biometric identification template and are transmitted from the first processor to the second processor, and

wherein the minutiae matching process is a second stage of the biometric identity authentication process to issue a biometric authentication result using the intermediate results.

39. (original) A method according to claim 38, wherein said process names include object names associated with respective object identifiers.

40. (original) A method according to claim 39, wherein each object has associated therewith a plurality of functions each identified by function names and associated function identifiers in the first and second task tables.

41. (previously presented) A method according to claim 38, wherein the process locator identifies the starting address of a process in a program memory.

42. (previously presented) A method according to claim 38, wherein the second processor has significantly less processing power than the first processor.

43. (previously presented) A method according to claim 38, wherein the second processor is arranged to execute locally processes requiring less processing power than those executed by the first processor.

44. (cancelled)

45. (previously presented) A method according to claim 38, wherein there are a plurality of second processors in communication with a single first processor, each second processor holding a respective task table, and the first

processor holding a first task table including all processes identified by the task tables of the second processors.

46. (previously presented) A method according to claim 38 , wherein a client bridge is connected between the first and second processors, the client bridge conveying said requests from the second processor to the first processor and returning the results from the first processor to the second processor.

47. (previously presented) A method according to claim 38, wherein the first processor is a client terminal and the second processor is embedded on a secure portable computing and data storage platform.

48. (previously presented) A method according to claim 38, wherein there are a plurality of first processors connected via a client bridge to one or more second processor and arranged to implement different subsets of the processes in the task table of the second processor.

49. (previously amended) A processing system comprising:

a first processor in which is stored a first task table containing a plurality of process names and process identifiers, each associated with a process locator;

a second processor in which is stored a second task table containing said process names with associated process identifiers;

the second processor including a distributed object execution manager for identifying a process to be executed and issuing a request to the first processor to execute said process; and

the first processor including a client distributed object execution manager for controlling the execution of said processes at the first processor, the results of execution of the processes implemented at the first processor being returned to the second processor;

wherein the first processor and the second processor are operable to execute an operation, the operation being a fingerprint-matching algorithm comprising a base minutiae finding process executed by the first processor and a minutiae matching process executed by the second processor,

wherein the base minutiae finding process is a first stage of a biometric identity authentication process implemented between data derived from a user biometric parameter and an open portion of a biometric identification template, wherein the biometric identification template is divided into the open portion and a secure portion, to produce intermediate results, said open portion containing a subset of minutiae data selected such that the content of the open portion is insufficient to construct a fake template that would allow an impostor to be incorrectly authenticated as a genuine user, and said intermediate results comprise parameters for alignment of said data and said biometric identification template and are transmitted from the first processor to the second processor, and

wherein the minutiae matching process is a second stage of the biometric identity authentication process to issue a

biometric authentication result using the intermediate results.

50. (original) A processing system according to claim 49, wherein the first processor includes a client manager for handling communications between the first and second processors.

51. (previously presented) A system according to claim 49, wherein the first processor includes an execution manager for handling the execution of processes.

52. (previously presented) A system according to claim 49, wherein the first processor comprises a program store for holding said processes, the process locator being used to identify the location of said processes in the program store.

53. (previously presented) A system according to claim 49, wherein the second processor includes a remote device manager for transmitting said requests to the first processor.

54. (previously presented) A system according to claim 49, wherein the second processor comprises a stack for holding results returned to it from the first processor.

55. (previously presented) A system according to claim 49, wherein the second processor includes a program store for holding said processes.

56. (previously presented) A system according to claim 49, wherein the first processor comprises a client terminal.

57. (previously amended) A system according to claim 49, which comprises a plurality of first processors, the system further

comprising a client bridge for handling communications between the first processors and the second processor.

58. (original) A system according to claim 57, wherein each first processor comprises a server.

59. (previously presented) A system according to claim 57, wherein the client bridge includes a network execution manager for transmitting requests from the second processor to the appropriate one of the first processors, based on a processor kdentifier in the request.

60. (previously amended) A system according to claim 49, comprising a plurality of second processors and a client bridge for connecting said second processors to said first processor.

61. (previously amended) A system according to claim 49, wherein the second or each second processor is embedded on a respective portable secure computing and data storage platform such as smart card.

Remarks

Claims 1, 2, 3, 5, 7 through 25, 27 and 29 through 43 and 45 through 61 remain pending in the application.

Claims 1, 2, 3, 5, 7 through 25, 27 and 29 through 37 stand rejected under 35 U.S.C. § 103(a) as unpatentable over Hamid, Method and Apparatus for Hashing Data, U.S. Patent 7,274,804 (Sep. 25, 2007), in view of Larsson, et al., Method and Device for Positioning a Finger when Verifying a Person's Identity, U.S. Patent Publication 2004/0215615 (Oct. 28, 2004). Applicants submit herewith a declaration under 37 C.F.R. 1.131 along with the original annotated source code (Exhibit 1), commented source code (Exhibit 2) and a screen shot (Exhibit 3) of the directory holding the source code. The declarant asserts and the exhibits support the assertion that the annotated source code (Exhibit 1) was prepared as discussed in the declaration and was operational in April 2001 showing actual reduction to practice of the claimed invention before the filing dates of any of the cited references. The commented source code (Exhibit 2) contains comments in bold prepared for the examiner's convenience to follow the claim limitations. The commented version of the source code clearly shows all the elements of the pending claims and thus fully supports the declaration of the inventor.

Larsson was filed July 5, 2001 and as the annotated source code (Exhibit 1) proves, the limitations of the present claims were incorporated in the source code in April 2001, several months before the filing of Larsson. Thus, Larsson is not available as prior art.

The actual reduction to practice also predates the filing date of Hamid and its parent application issued to Hillhouse, et al., Method and Apparatus for Supporting a Biometric Registration Performed on a Card, U.S. Patent 7,274,807 (Sep. 25, 2007) (Hereinafter Hillhouse). The priority date of Hillhouse is May 30, 2002. Accordingly, even Hillhouse (of which the cited Hamid reference is a CIP) is not prior art. Thus, neither Hamid nor its parent, Hillhouse, are available for use as prior art in rejecting the claims of the present application. Accordingly, Applicants respectfully request that the rejections of claims 1, 2, 3, 5, 7 through 25, 27 and 29 through 37 be withdrawn.

Claims 38 through 43 and 45 through 61 stand rejected under 35 USC § 103(a) as unpatentable over Studd, Method and System for Executing Applications on a Mobile Device, U.S. Patent Application Publication 2004/0122774 (Jun. 24, 2004) in view of Hamid and further in view of Larsson. As discussed above, Larsson is not available as prior art and thus this rejection should be withdrawn. The earliest priority date for Studd is August 2, 2002 over a year after the date of applicant's actual reduction to practice. Thus, Studd is also not available as prior art and this rejection should be withdrawn.

Conclusion

This response has addressed all of the Examiner's grounds for rejection. The rejections based on prior art have been traversed. Reconsideration of the rejections and allowance of the claims is requested.

Date: November 22, 2010 By: /Paul J. Backofen/
Paul J. Backofen, Esq.
Reg. No. 42278